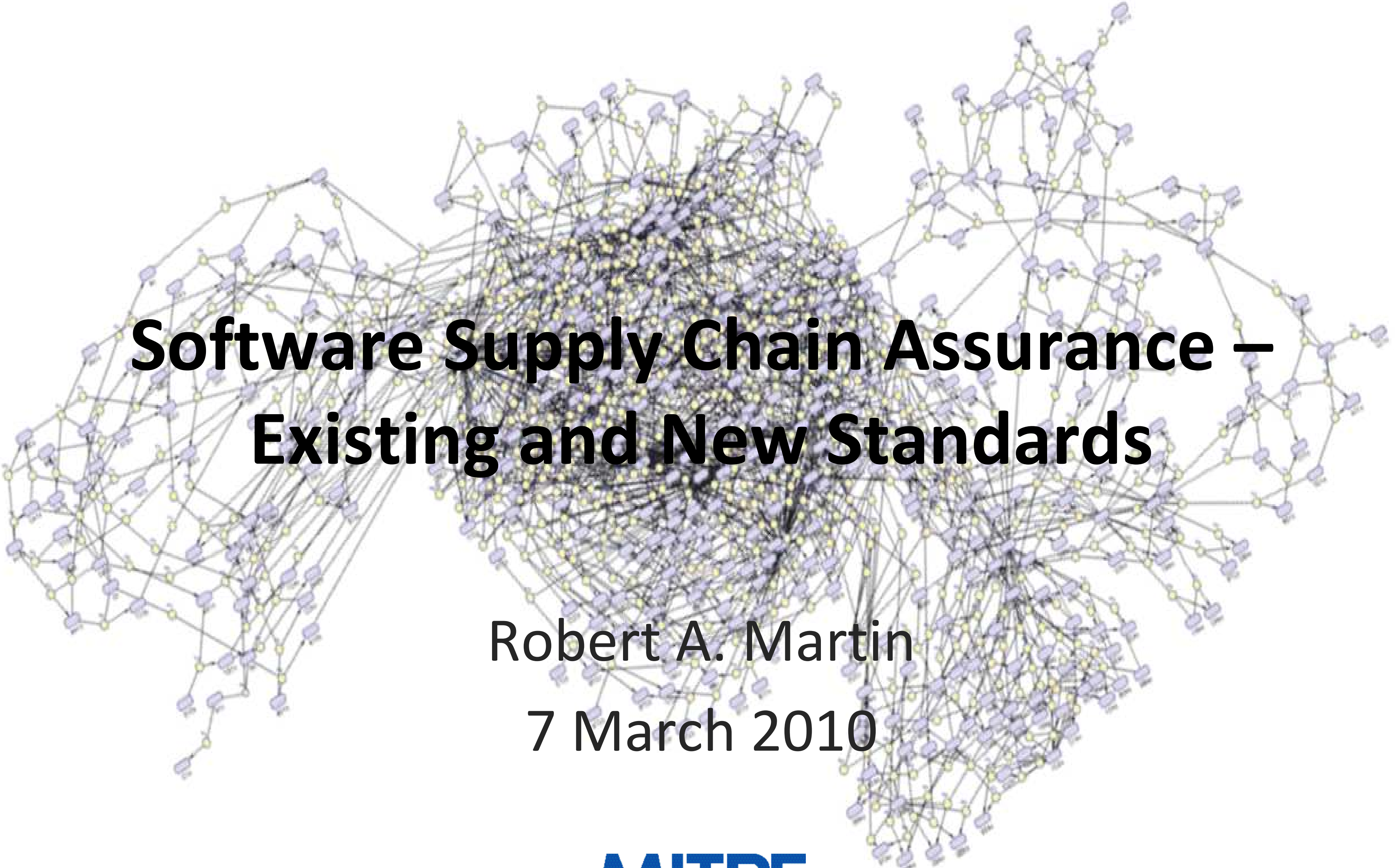


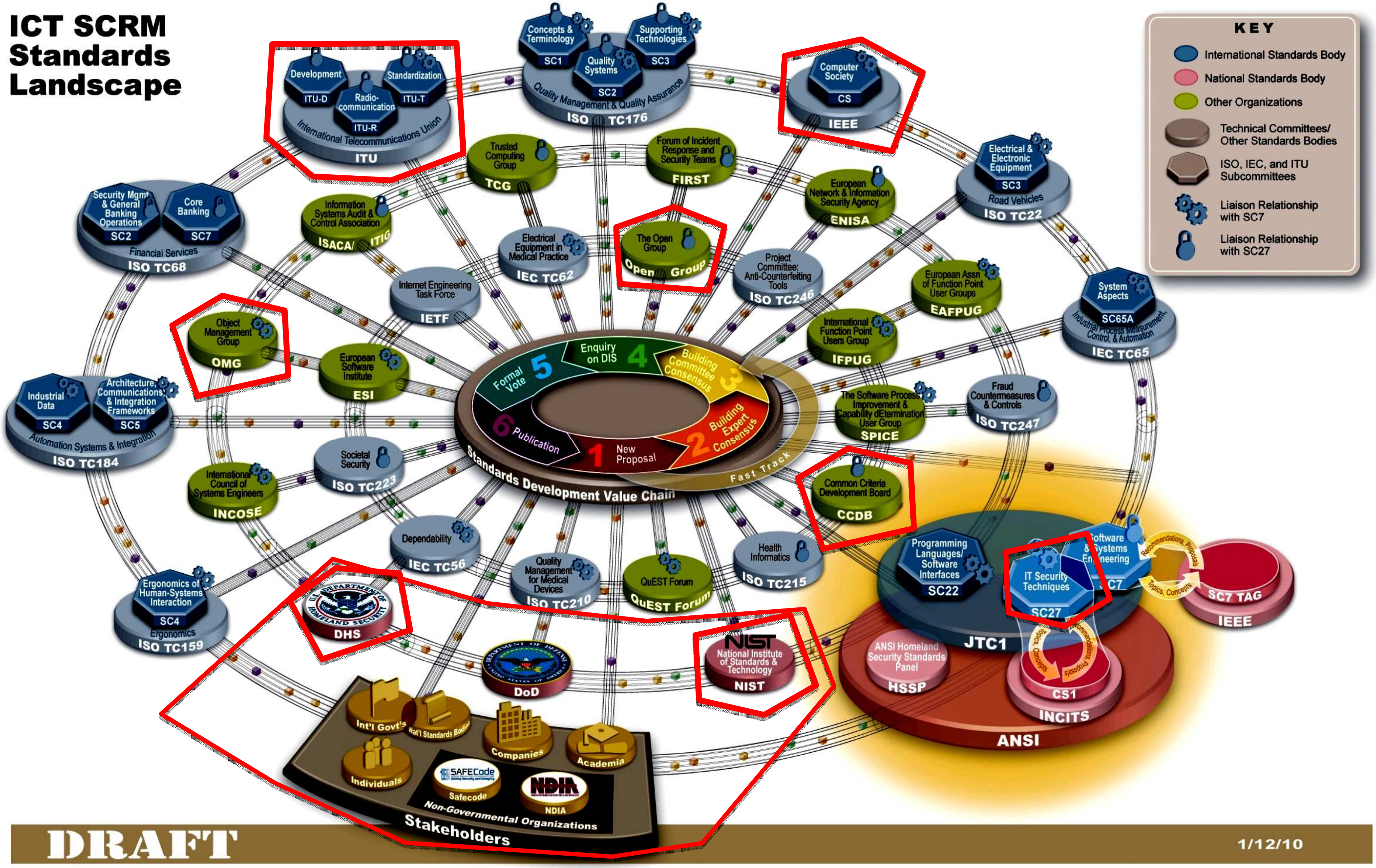
Software Supply Chain Assurance – Existing and New Standards

Robert A. Martin

7 March 2010

MITRE

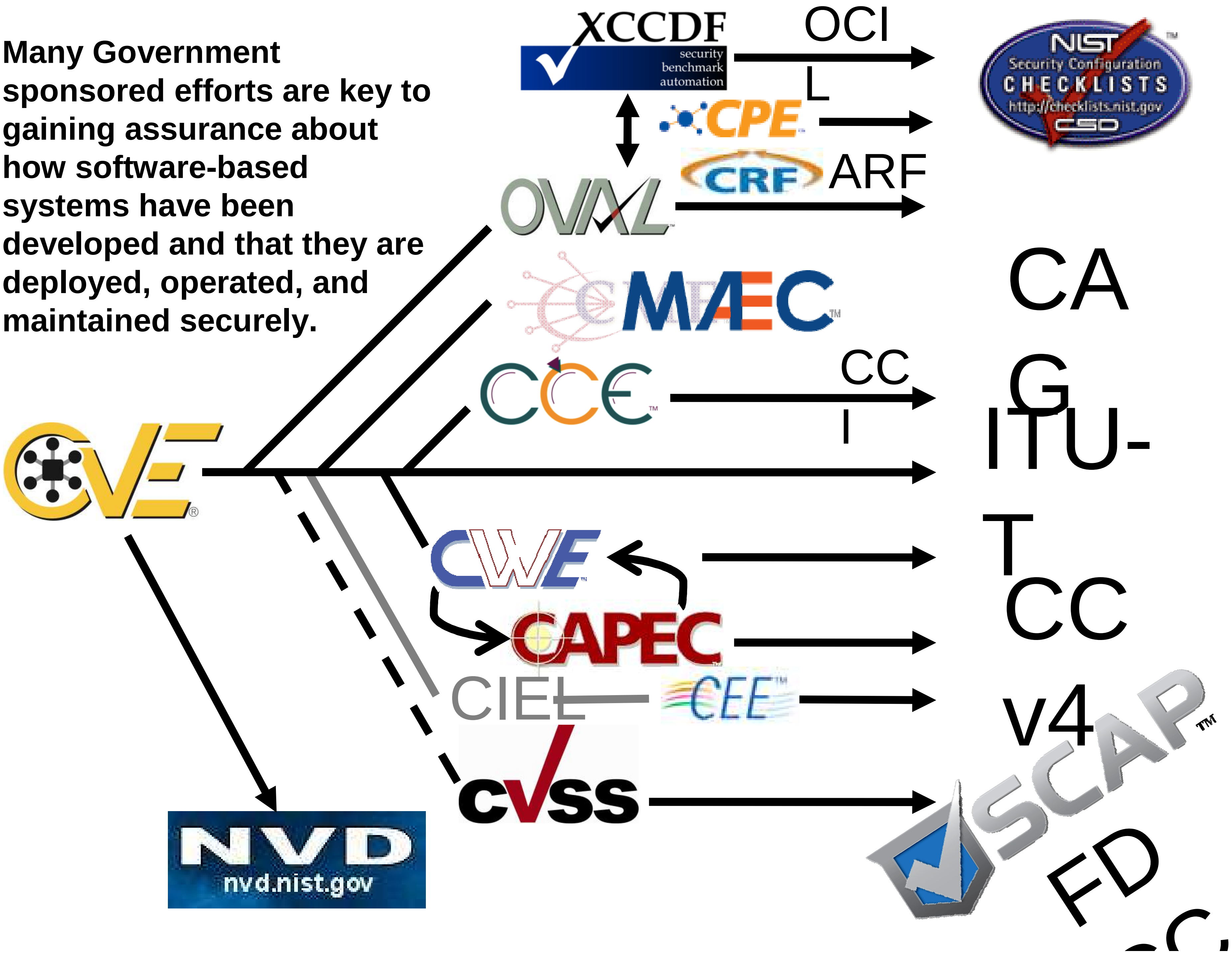
ICT SCRM Standards Landscape


KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees/ Other Standards Bodies
ISO, IEC, and ITU Subcommittees
Liaison Relationship with SC7
Liaison Relationship with SC27
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Information Systems Audit & Control Association
ISACA/ITIG
Electrical Equipment in Medical Practice
IEC TC62
The Open Group
Open Group
Project Committee: Anti-Counterfeiting Tools
ISO TC246
European Assn of Function Point User Groups
EAFPUG
Internet Engineering Task Force
IETF
Object Management Group
OMG
European Software Institute
ESI
International Function Point Users Group
IFPUG
Industrial Data
SC4
Architecture, Communications, & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Enquiry on DIS
4
Building Committee Consensus
3
Formal Vote
5
Publication
6
New Proposal
1
Building Expert Consensus
2
Fast Track
Standards Development Value Chain
The Software Process Improvement & Capability dEtermination User Group
SPICE
Fraud Countermeasures & Controls
ISO TC247
Societal Security
ISO TC223
International Council of Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
Health Informatics
ISO TC215
Programming Languages, Software Interfaces
SC22
Software & Systems Engineering
SC7
IT Security Techniques
SC27
JTC1
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
U.S. DEPARTMENT OF HOMELAND SECURITY
DHS
DoD
NIST
National Institute of Standards & Technology
NIST
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

DRAFT

1/12/10

Many Government sponsored efforts are key to gaining assurance about how software-based systems have been developed and that they are deployed, operated, and maintained securely.



Industry, Government, and Academia

CAPEC

MAE
C

CWE

CVSS

ARF

OCI
L

OVAL

CPE

XCCDF
security
benchmark
automation

CEE

NVD
nvd.nist.gov

CVE

NIST
Security Configuration
CHECKLISTS
http://checklists.nist.gov
CSD

U.S. Department of Homeland Security
DHS
Department of Defense United States of America
DoD
NIST
National Institute of Standards & Technology
NIST
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

FD
CC

SCAP™

EMAP

SwAAP

NIST Special Publications:

SP800-36	CVE
SP800-40	CVE, OVAL
SP800-42	CVE
SP800-44	CVE
SP800-51	CVE
SP800-53a	CVE, OVAL, CWE
SP800-61	CVE, OVAL
SP800-70	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-82	CVE
SP800-86	CVE
SP800-94	CVE
SP800-115	CVE, CCE, CVSS, CWE
SP800-117	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-126	CVE, OVAL, CCE, CPE, XCCDF, CVSS

NIST Interagency Reports:

NISTIR-7007	CVE
NISTIR-7275	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7435	CVE, CVSS, CWE
NISTIR-7511	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7517	CVE
NISTIR-7581	CVE
NISTIR-7628	CVE, CWE

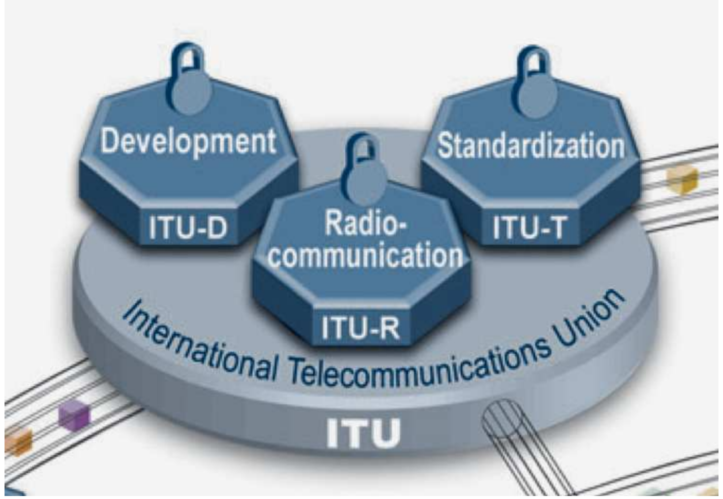
FD

CC

SCAP™

EMAP

SwAAP

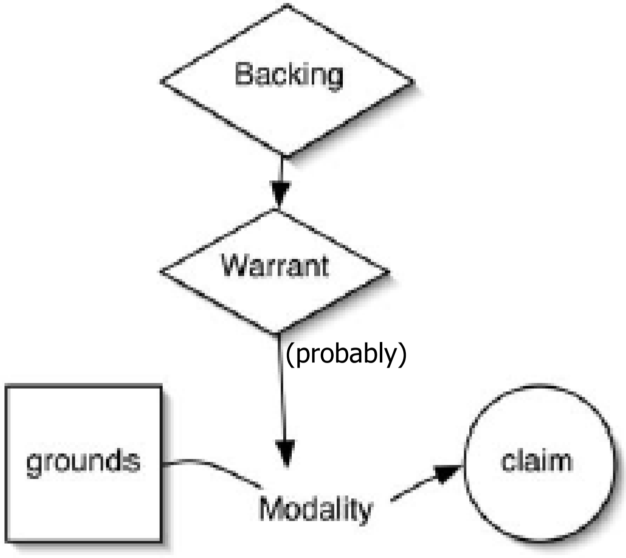


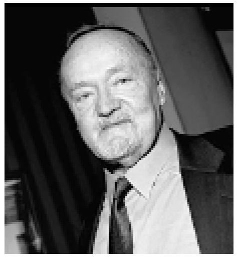
ITU-T Study Group 17 Question 4 – Cyber Security
Cyber Security Exchange Framework (CYBEX)

Creating x.series standards to capture the correct and supported USE of the enumerated concepts and languages – effort stewardship and definition stays with originating organizations

Identifier	Title	Current Text
X.cybief	Cybersecurity Information Exchange Framework	TD406
X.cybief.1	Guidelines for Administering the OID arc for cybersecurity information exchange	TD406
X.cce	**Common Configuration Enumeration**	TD406
X.cee	**Common Event Expression**	TD406
X.chirp	Cybersecurity Heuristics and Information Request Protocol	TD406
X.cpe	**Common Platform Enumeration**	TD406
X.crf	**Common Result Format**	TD406
X.cve	**Common Vulnerabilities and Exposures**	TD405
X.cvss	**Common vulnerability scoring system**	TD412
X.cwe	**Common Weakness Enumeration**	TD406
X.cwss	**Common Weakness Scoring System**	TD406
X.dexf	Digital evidence exchange file format	C97
X.dpi	Deep Packet Inspection Exchange Format	TD406
X.gridf	SmartGrid Incident Exchange Format	TD406
X.oval	**Open Vulnerability and Assessment Language**	TD406
X.pfoc	Phishing, Fraud, and Other Crimeware Exchange Format	TD406
X.scap	**Security Content Automation Protocol**	TD406
X.teef	Cyber attack tracing event exchange format	C135, C129
X.xccdf	**eXensible Configuration Checklist Description Format**	TD406
X.cybief-[namespace],	Cybersecurity Information Exchange Namespace	C148
X.cybief-discovery	Cybersecurity Information Exchange Discovery	C145
X.capec	**Common Attack Pattern Enumeration and Classification**	TD406
X.iodef	Incident Object Description Exchange Format	TD406

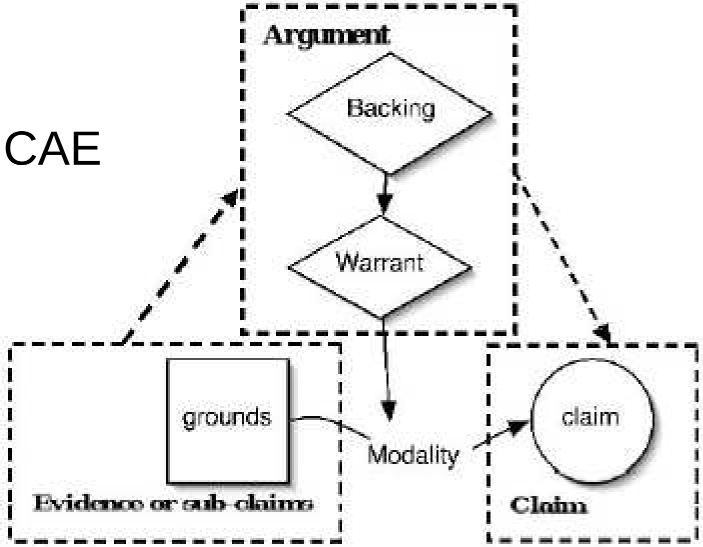
Assurance Claims with Support by ‘Substantial’ Reasoning

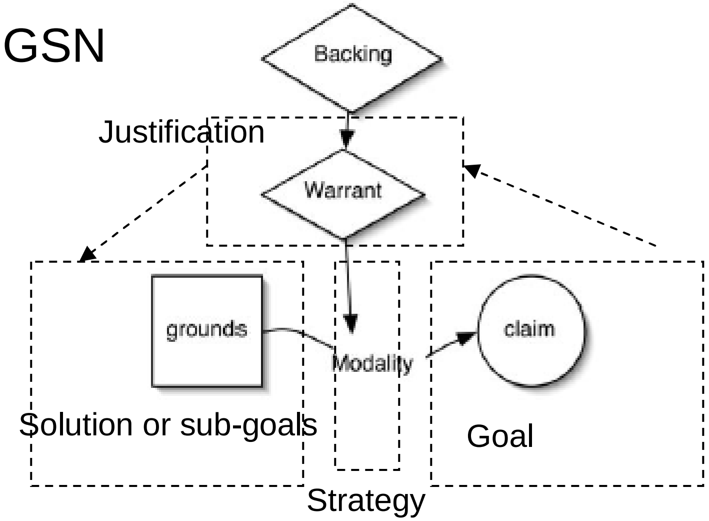




Stephen Toulmin, 1958

- Claims are assertions put forward for general acceptance
- The justification for claim is based on some grounds, the “specific facts about a precise situation that clarify and make good for a claim”
- The basis of the reasoning from the grounds (the facts) to the claim is articulated. These are statements indicating the general ways of argument being applied in a particular case and implicitly relied on and whose trustworthiness is well established”



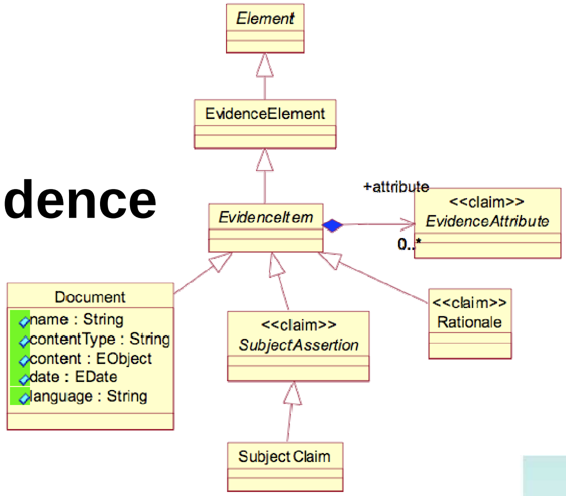


System Assurance (SySA) Task Force

- Software Assurance Evidence MetaModel (SAEM)
- Argumentation MetaModel (ARM)

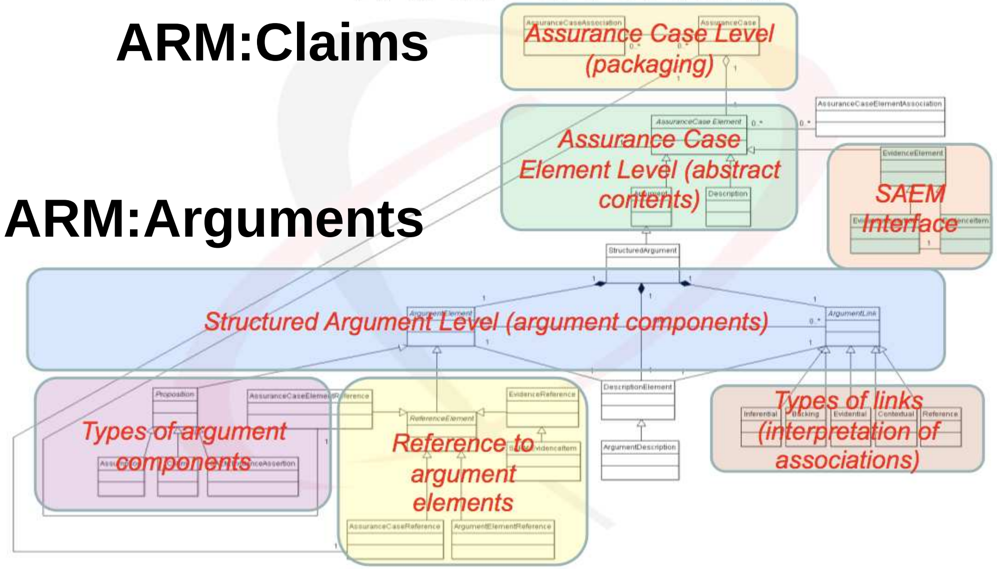
→ Coordinating with ISO/IEC 15026 part 2’s definition of “the Assurance Case”

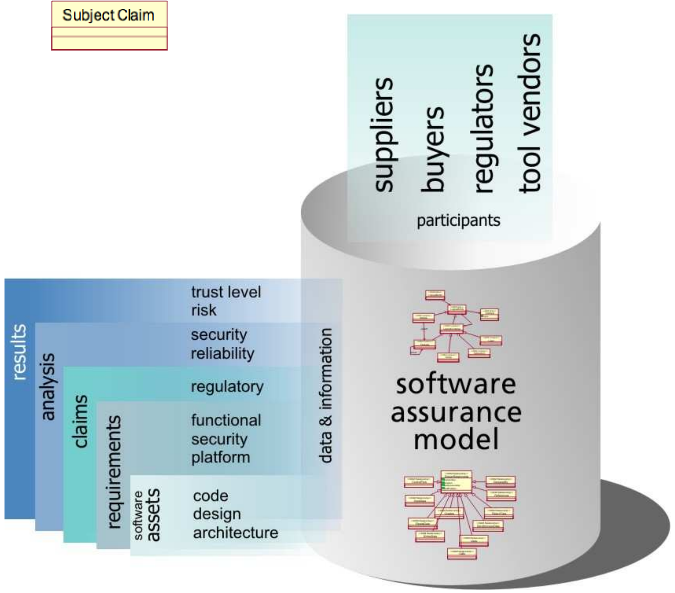
SAEM: Evidence



ARM:Claims

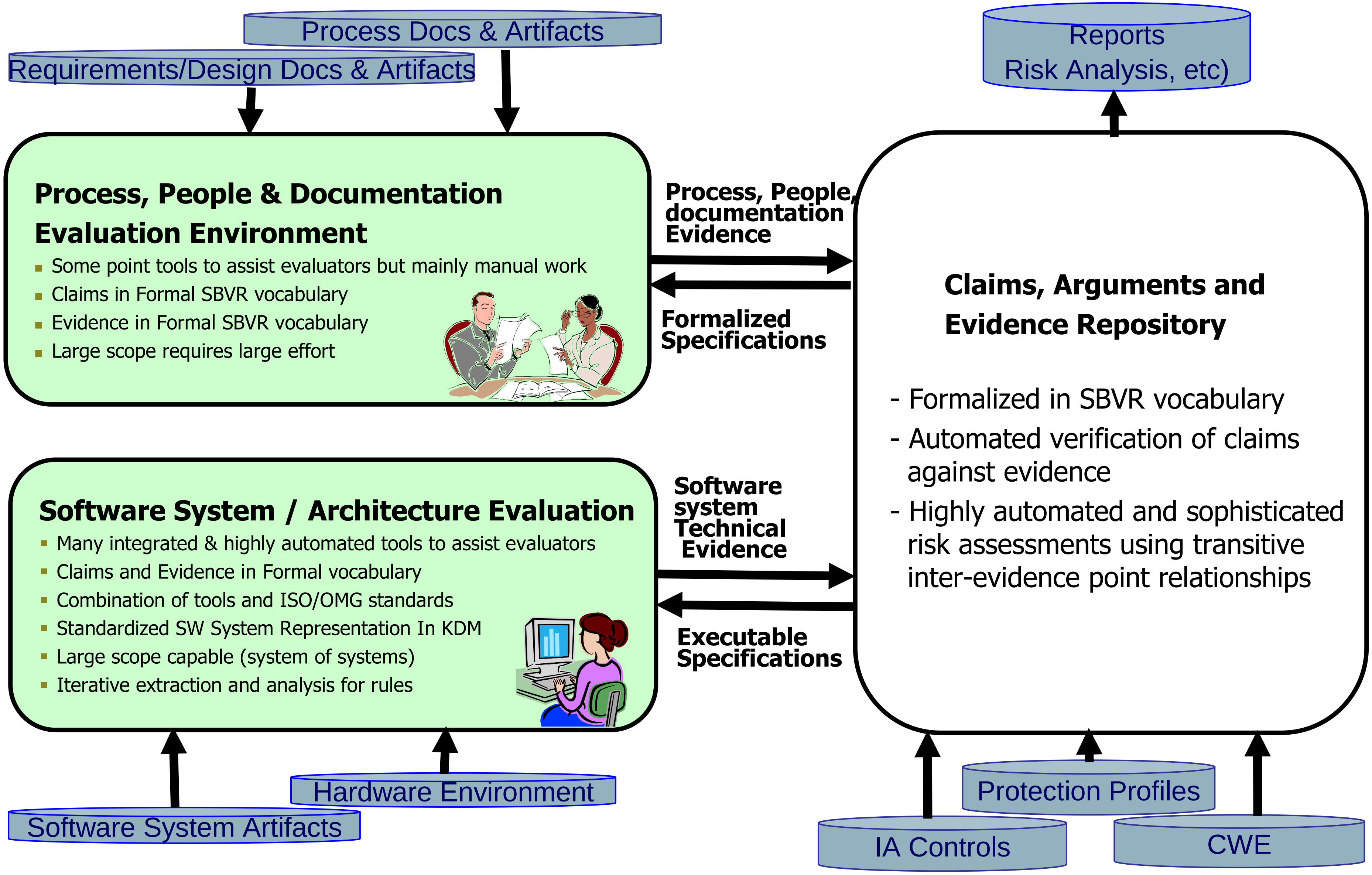
ARM:Arguments


Assurance Case Level (packaging)
Assurance Case Element Level (abstract contents)
SAEM Interface
Structured Argument Level (argument components)
Types of argument components
Reference to argument elements
Types of links (interpretation of associations)



Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related software system process, people and documentation



Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports
Risk Analysis, etc)

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort

Process, People, documentation Evidence

Formalized Specifications

Claims, Arguments and Evidence Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Software system Technical Evidence

Executable Specifications

Hardware Environment

Software System Artifacts

Protection Profiles

IA Controls

CWE

The Open Group
Open Group
U.S. Department of Homeland Security
DHS
Department of Defense United States of America
DoD
NIST
National Institute of Standards & Technology
NIST
Object Management Group
OMG

CWE Validation
Effectiveness Testing - ?

CWE
Compatibility and Effectiveness

CWEs with WhiteBox Definitions

Center For Assure SW
Tool Evaluation 2007
Tool Evaluation 2009

IARPA
STONESOUP- Securely Taking On New Executable Stuff Of Uncertain Provenance

OSD/NII
CWE Formalization

NIST SAMATE
SP 500-267
SP 500-269
SP 500-270

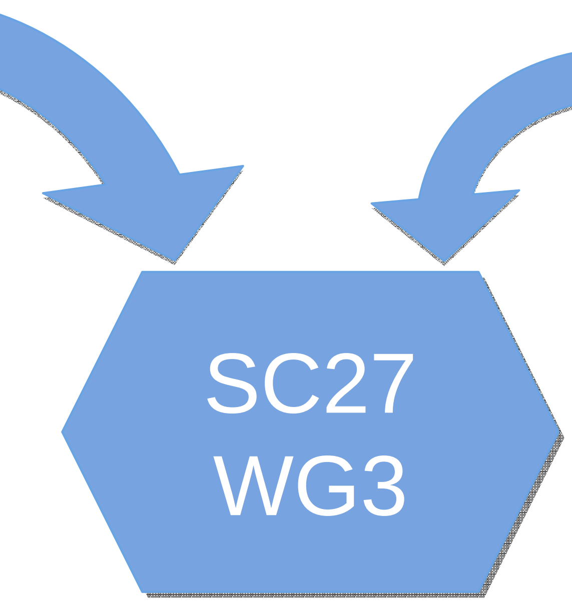
SAMATE Repository Dataset (SRD)

Automated Test Case Generator

NIST SATE
SATE08
SATE09

SySA Task Force
WhiteBox Definitions-to-SBVR-to-microKDM

All of these are aimed at different aspects of understanding how well tools find CWEs in software applications and what can be done to improve that and standardize the process for expressing a tools capabilities.

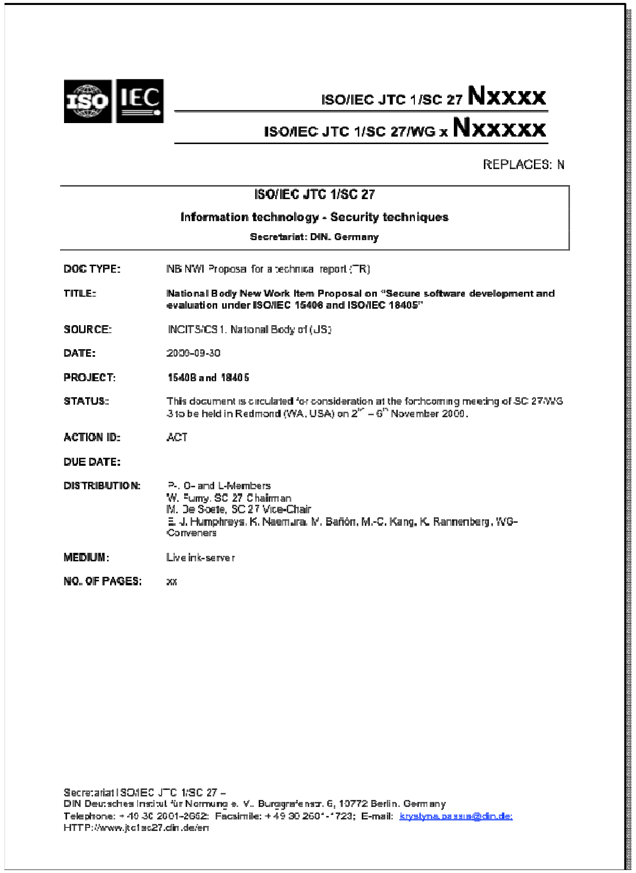


Common Criteria v4 CCDB

- TOE to leverage CAPEC & CWE
- Also investigating how to leverage ISO/IEC 15026

NIAP Evaluation Scheme

- Above plus
- Also investigating how to leverage SCAP



ISO/IEC JTC 1/SC 27 **Nxxxx**

ISO/IEC JTC 1/SC 27/WG x **Nxxxxx**

REPLACES: N

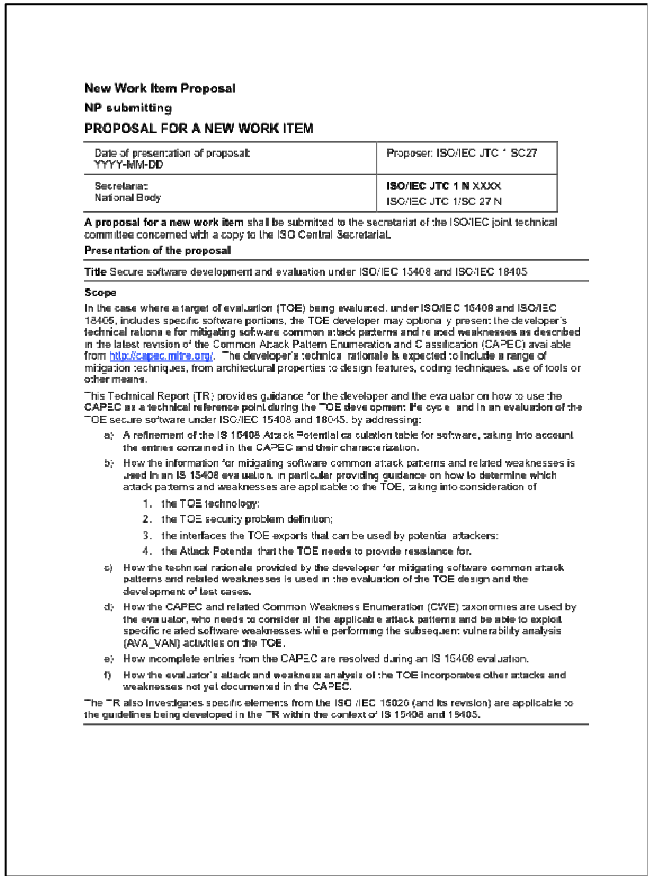
ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN. Germany

DOC TYPE:	NB NWI Proposal for a technical report (TR)
TITLE:	**National Body New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405"**
SOURCE:	INCITS/CS1. National Body of (US)
DATE:	2000-09-30
PROJECT:	**15408 and 18405**
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 27/WG 3 to be held in Redmond (WA, USA) on 2nd – 6th November 2000.
ACTION ID:	ACT
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy. SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys. K. Naemura. M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin. Germany
Telephone: +49 30 2601-2652; Facsimile: +49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en



New Work Item Proposal

NP submitting

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: YYYY-MM-DD	Proposer: ISO/IEC JTC 1 SC27
Secretariat: National Body	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 27 N

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405

Scope

In the case where a target of evaluation (TOE) being evaluated. under ISO/IEC 15408 and ISO/IEC 18405, includes specific software portions, the TOE developer may optionally present the developer's technical rationale for mitigating software common attack patterns and related weaknesses as described in the latest revision of the Common Attack Pattern Enumeration and Classification (CAPEC) available from http://capec.mitre.org/. The developer's technical rationale is expected to include a range of mitigation techniques, from architectural properties to design features, coding techniques, use of tools or other means.

This Technical Report (TR) provides guidance for the developer and the evaluator on how to use the CAPEC as a technical reference point during the TOE development life cycle and in an evaluation of the TOE secure software under ISO/IEC 15408 and 18045. by addressing:

a) A refinement of the IS 15408 Attack Potential calculation table for software, taking into account the entries contained in the CAPEC and their characterization.

b) How the information for mitigating software common attack patterns and related weaknesses is used in an IS 15408 evaluation. in particular providing guidance on how to determine which attack patterns and weaknesses are applicable to the TOE, taking into consideration of

   1. the TOE technology;
   2. the TOE security problem definition;
   3. the interfaces the TOE exports that can be used by potential attackers;
   4. the Attack Potential that the TOE needs to provide resistance for.

c) How the technical rationale provided by the developer for mitigating software common attack patterns and related weaknesses is used in the evaluation of the TOE design and the development of test cases.

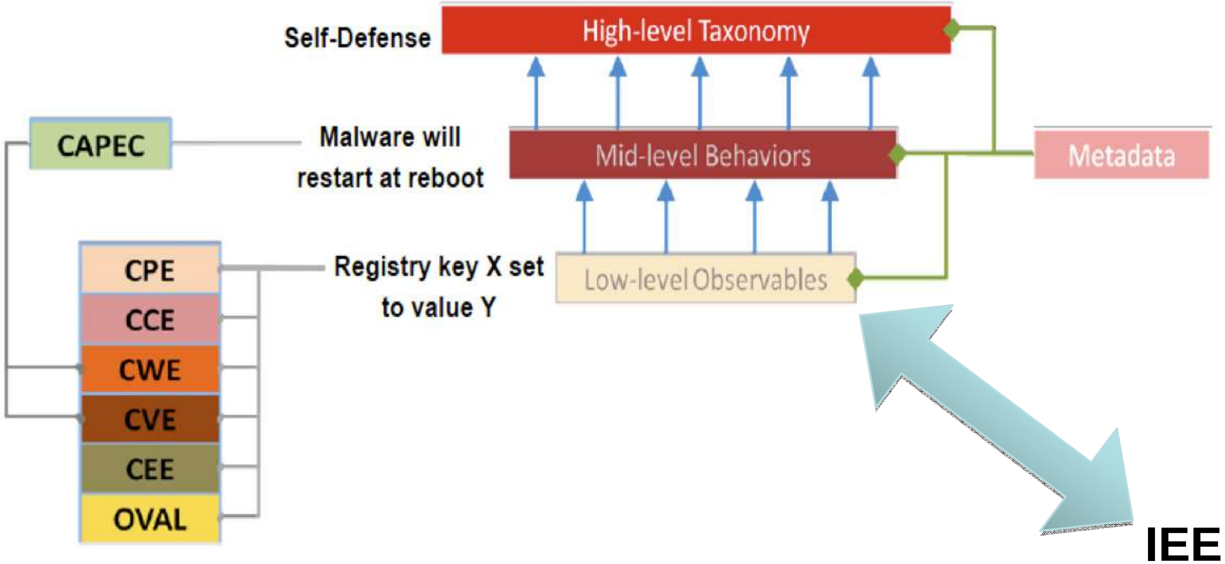
d) How the CAPEC and related Common Weakness Enumeration (CWE) taxonomies are used by the evaluator, who needs to consider all the applicable attack patterns and be able to exploit specific related software weaknesses while performing the subsequent vulnerability analysis (AVA_VAN) activities on the TOE.

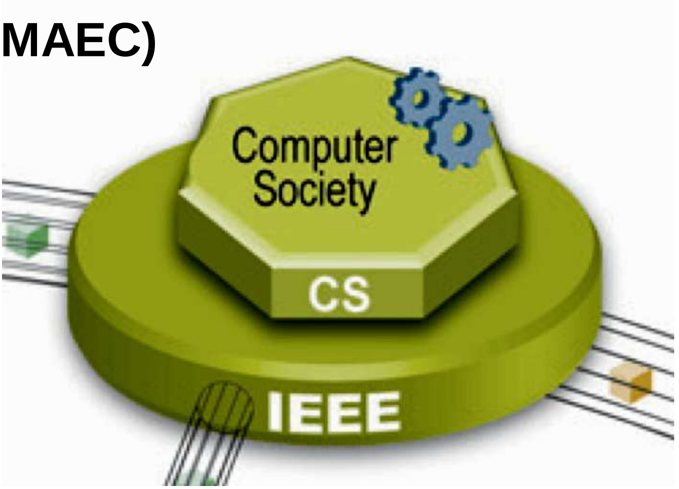
e) How incomplete entries from the CAPEC are resolved during an IS 15408 evaluation.

f) How the evaluator's attack and weakness analysis of the TOE incorporates other attacks and weaknesses not yet documented in the CAPEC.

The TR also investigates specific elements from the ISO/IEC 15026 (and its revision) are applicable to the guidelines being developed in the TR within the context of IS 15408 and 18405.

Malware Attribute Enumeration and Characterization (MAEC)



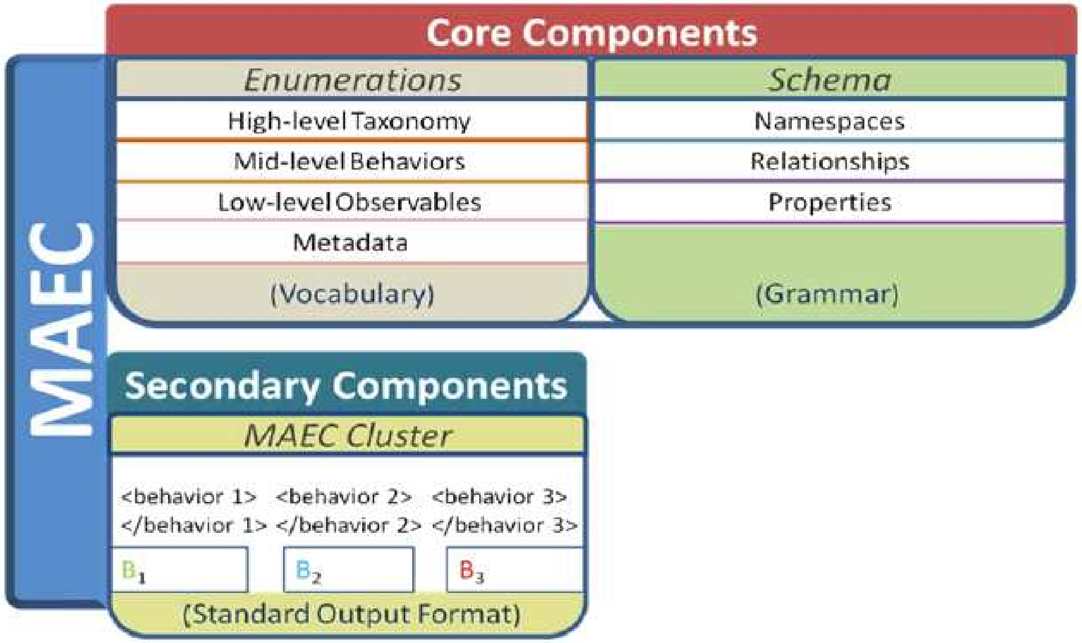


IEEE's Industry Connections Security Group (ICSG)

First working group is focused on malware (malicious software such as viruses, worms and spyware).

Microsoft, McAfee, Symantec, Sophos, AVG, and Trend

MAEC High-level Overview



MAEC

Core Components

Enumerations

High-level Taxonomy

Mid-level Behaviors

Low-level Observables

Metadata

(Vocabulary)

Schema

Namespaces

Relationships

Properties

(Grammar)

Secondary Components

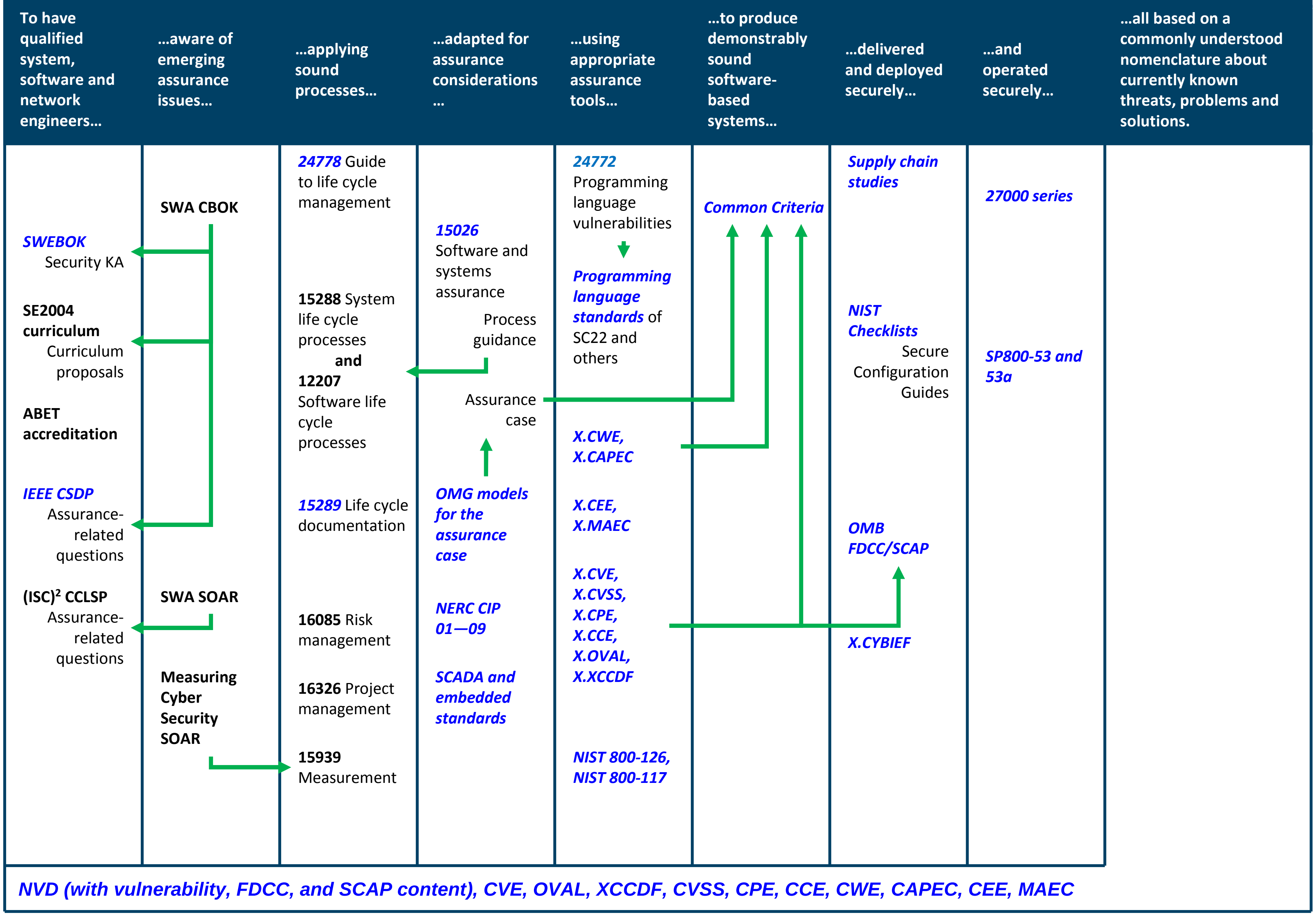
MAEC Cluster

```
<behavior 1>  <behavior 2>  <behavior 3>
</behavior 1> </behavior 2> </behavior 3>
```

B_1 B_2 B_3

(Standard Output Format)

The GOAL of Cyber Security and Assurance Standards



To have qualified system, software and network engineers…	…aware of emerging assurance issues…	…applying sound processes…	…adapted for assurance considerations …	…using appropriate assurance tools…	…to produce demonstrably sound software-based systems…	…delivered and deployed securely…	…and operated securely…	…all based on a commonly understood nomenclature about currently known threats, problems and solutions.
SWEBOK Security KA **SE2004 curriculum** Curriculum proposals **ABET accreditation** ***IEEE CSDP*** Assurance-related questions **(ISC)^2 CCLSP** Assurance-related questions	**SWA CBOK** **SWA SOAR** **Measuring Cyber Security SOAR**	*24778* Guide to life cycle management **15288** System life cycle processes **and 12207** Software life cycle processes *15289* Life cycle documentation **16085** Risk management **16326** Project management **15939** Measurement	***15026*** Software and systems assurance Process guidance Assurance case ***OMG models for the assurance case*** ***NERC CIP 01—09*** ***SCADA and embedded standards***	***24772*** Programming language vulnerabilities ***Programming language standards*** of SC22 and others ***X.CWE, X.CAPEC*** ***X.CEE, X.MAEC*** ***X.CVE, X.CVSS, X.CPE, X.CCE, X.OVAL, X.XCCDF*** ***NIST 800-126, NIST 800-117***	***Common Criteria***	***Supply chain studies*** ***NIST Checklists*** Secure Configuration Guides ***OMB FDCC/SCAP*** ***X.CYBIEF***	***27000 series*** ***SP800-53 and 53a***	

NVD (with vulnerability, FDCC, and SCAP content), CVE, OVAL, XCCDF, CVSS, CPE, CCE, CWE, CAPEC, CEE, MAEC